Prioritizing Human Interface Design Issues for Range Safety Systems using Human Factors Process FMEA

David C. Dunkle
ITT Industries – Systems Division

Range Safety System Modernization

- Many of the AF Range (Eastern and Western) systems are undergoing a modernization
- Systems that receive telemetry data and others that provide flight termination functions are being modernized.
- A major aspect in the design of these systems is a focus on the human element in system performance.
- The WCCS is among the first systems being developed in this effort.

Safety System modernization to support launches is underway

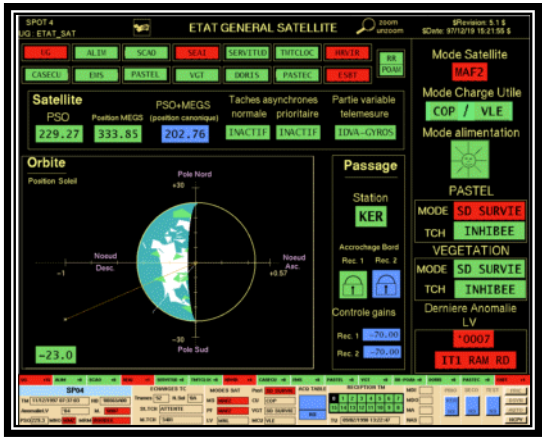
What is the WCCS?

- The Western Range Operations Control Center (WROCC) monitors safety and performance aspects of Western range space launches
- The WROCC Command Control System (WCCS) is used to provide a destruct signal to launch vehicles in hazardous situations.
- The control for sending the command destruct signal is assigned to the Mission Flight Control Officer (MFCO).

WCCS provides functionality to destruct unsafe launches

WCCS User Interface *(examples)*

- Operator Interface for monitoring system performance



- MFCO command panel for initiating the destruct command

User Interfaces for WCCS are HW- and SW- based

Safety Critical Aspect of WCCS

- A critical aspect of Range Safety systems is to monitor launches and provide a method for controlling errant vehicle flight, to minimize risks to general public
- Following lift-off, the only way for Range Control to terminate an unsafe vehicle is through the Command Destruct system
- Consequently, failure of the system could result in personnel or equipment damage.
- Safety critical system development follows strict rules for reliability requirements and safety analyses

WCCS complies with strict safety critical requirements

Analysis Requirements For WCCS

- Design must comply with Command Destruct System Range Safety requirements
- Preliminary Hazard Analysis
  - To include human factors engineering, human error analysis of operator functions, tasks and requirements…
- Sub-System Hazard Analysis
  - To include the human as a component within a subsystem, modes of failure including human errors…
- These analyses will include hardware, software, and human hazards.

Hazard Analyses include a comprehensive list of possible errors

Human Factors Process FMEA

- The HF PFMEA provides a systematic method to analyze and mitigate the risk of human error in a performance of tasks.
- FMEA (Failure Modes and Effects Analysis) typically analyzes system hardware for possible failure modes and “worst case” effects.
- Process FMEA analyzes the system’s processes rather than specific pieces of equipment.
- HF PFMEA analyzes tasks within a process to identify human errors that may lead to failures, and the “worst case” effects on the system.

HF PFMEA analyzes the human aspects of system failures

Human Factors Process FMEA Philosophy

- The HF PFMEA is based on the philosophy that human error can be controlled by:
  - Managing the performance shaping factors effecting human performance
  - Building barriers to prevent human error
  - Adding controls to detect and correct human error before it leads to an undesirable outcome
  - Building fault tolerant systems

Human Error must be accounted for and can be controlled

Benefits of HF PFMEA

- A generic method that can be applied to a variety of processes
- Identifies human errors that can become single points of failure
- Determines which potential human errors are the most critical by revealing the severity and likelihood of occurrence.
- Provides recommendations for human error management

HF PFMEA generates solutions to human error problems

Conducting a HF PFMEA

- Describe Mission
  - Begin with the Result
  - Describe a Properly Operating process
- Define Process Flow
  - Simple Block Diagram
- Identify Human-System Interfaces
  - Could be:
    - Human/Machine
    - Human/Computer
    - Human/Document
    - Etc…

Initial steps require a solid concept of operations

Conducting a HF PFMEA (cont.)

- Task Analysis
  - Critical Part of Analysis
  - Depth of Analysis differs from Human Factors Procedures MIL-HDBK-46855A
  - Important to capture all tasks (explicit steps) and subtasks (implicit steps)

- Identify Potential Errors
  - Three Basic Types
    - Perception – Decision-Making – Action
  - Errors of Omission and Commission
  - Focus on human errors within a correctly operating system

A well-documented Task Analysis is essential to the HF PFMEA

Conducting a HF PFMEA (cont.)

- Identify the Performance Shaping Factors
  - Factors that influence the tendency to error
  - Requires observation and/or analysis to identify

- Identify Barriers to Prevent Error
  - Error-specific
  - Prevent or eliminate the likelihood of error
  - Examples are lockouts, shields, selector limits, data filters, etc…

- Determine the Likelihood of Errors
  - Consider task-specific environment
  - Inputs include actual event data, human error literature, domain expert judgment.

The possibility of human error is determined by several variables

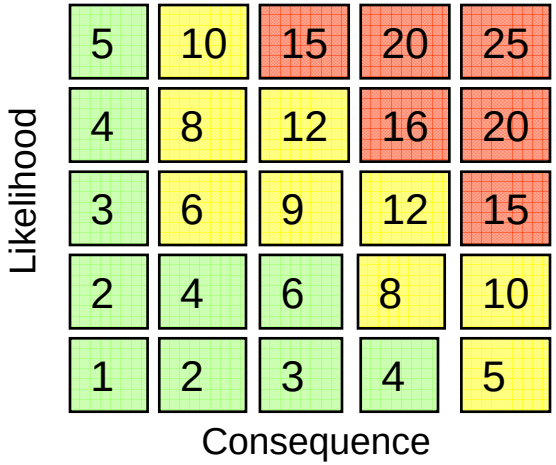
Conducting a HF PFMEA (cont.)

- Identify Error Controls
  - Detection and correction of error before it becomes a hazard
  - Examples are Alarms, Peer reviews, Activity Feedback.
- Determine Potential Effects of Errors
  - Analyze for “Worst Case” effects
- Evaluate Risk (Likelihood X Consequence)
  - Estimating Risk includes likelihood of error, effects of controls, any downstream conditions
  - Estimating Consequence involves the severity of “Worst case” scenario
- Generate Solutions for Human Interface Priorities

HF PFMEA provides usable results to improve the system design

Prioritizing Design Improvements

- Risk Assessment provides a numerical Risk Assessment Code (RAC) to focus design improvements
  - A score of 15 or above requires a design change
  - A score of ~ 6 or below does not require a change



- Generate Solutions for Human Interface Priorities
  - Reduce rate of error, detect and correct error, use redundant systems

HF PFMEA provides usable results to improve the system design

Mechanics of the HF PFMEA

- Consuming aspects of the analysis are the Task Analysis and Evaluation of Risk
  - Task Analysis requires in-depth knowledge of operator actions
  - Evaluation of Risk requires in-depth knowledge of system functionality

- Focusing Analysis on Safety-Critical functions is important
  - Resulting analysis contained 100 pages and over 500 error criticality ratings.

HF PFMEA is not a quick-&-dirty analysis

Results of HF PFMEA

- Errors associated with MFCO command activation were highest-rated risks
  - Inadvertent command initiation
  - Delayed or No command initiation

- Barriers and coding methods were provided as system design improvements

- Further refinement of HF PFMEA will focus on possible configuration errors.

HF PFMEA provides excellent rationale for design improvements

Lessons Learned Along the Way

- Identify process errors, PSFs, Barriers, Controls, etc., in groups
  - Paper notes support computer-based tool for analysis development
- Complete entire HF PFMEA step before moving to next step
  - Sequence allows for focus on step rather than result (end justifying the means).
- As with any Task Analysis, operational validation is necessary for a useful result
  - Actual operators must review tasks
- Nearly any significant process can be expanded to fill hundreds of pages of HF PFMEA analysis.
  - Scope of analysis is critical to valuable results.

Follow the HF PFMEA Process

Tools for Completing an HF PFMEA

- Training
  - NASA 1.1 Human Factors Process FMEA course

- Relex Professional HF module
  - Automates redundant steps, calculates LOE's, etc.
  - Provides a standardized method for completion, and result format.

Train and Tools are available for HF PFMEA